

p -adic exponential ring, p -adic Schanuel's conjecture and decidability

Nathanaël Mariaule

Abstract

Let $\exp(x)$ be the power series $\sum x^n/n!$. Then $E_p(x) := \exp(px)$ (if $p \neq 2$, we set $E_2(x) = \exp(4x)$) is well-defined on \mathbb{Z}_p and determines a structure of exponential ring. In this paper, we prove that if a p -adic version of Schanuel's conjecture is true then the theory of $(\mathbb{Z}_p, +, \cdot, 0, 1, E_p)$ is decidable.

1 Introduction

Exponential rings and fields are well-established topics in model-theory. While the real exponential field \mathbb{R}_{\exp} and the complex exponential field \mathbb{C}_{\exp} have been studied by many people, there is pretty much nothing known about the p -adic numbers in the context of exponential fields. Note that there is no clear structure of exponential field attached to \mathbb{Q}_p . It is not hard to show that the natural exponential map $\exp(x)$ determined by the power series $\sum x^n/n!$ is convergent iff $v_p(x) > 1/(p-1)$. As there is no analytic continuation for analytic functions in \mathbb{Q}_p , we cannot extend $\exp(x)$ to a natural exponential function on \mathbb{Q}_p . However, we can use $\exp(x)$ to define a structure of exponential ring on \mathbb{Z}_p : let E_p be the map $x \mapsto \exp(px)$ (if $p \neq 2$, we set $E_2(x) = \exp(4x)$). Then E_p is convergent on \mathbb{Z}_p and $(\mathbb{Z}_p, +, \cdot, 0, 1, E_p)$ is an exponential ring i.e. E_p is a morphism of group from $(\mathbb{Z}_p, +, 0)$ to $(\mathbb{Z}_p^\times, \cdot, 1)$. Let us remark that the choice of E_p is not really canonical: we could have taken $\exp(tx)$ for any t with positive valuation.

Let \mathcal{L}_{\exp} be the language $(+, \cdot, 0, 1, E_p)$ and $\mathbb{Z}_{p,\exp}$ be the \mathcal{L}_{\exp} -structure with underlying set \mathbb{Z}_p and natural interpretation for the elements of the language. We call this structure the p -adic exponential ring. $\mathbb{Z}_{p,\exp}$ can be thought as a p -adic equivalent to the structures \mathbb{C}_{\exp} and \mathbb{R}_{\exp} (or to be more precise we should consider these structure with the domain of the exponential map reduced to a compact set). Very few results are known about $\mathbb{Z}_{p,\exp}$. In [2][3], A. Macintyre investigates for the first time the structure of p -adic exponential ring. He solves some decisions problem (decision problem for the positive universal part of the theory and for one variable existential sentences). In [1], he also gives a result of model-completeness whose an effective version was proved in [7] and will be usefull for this paper.

In this paper, we consider the question of the full decidability of the theory of $\mathbb{Z}_{p,\exp}$. It is well-known that the theory of \mathbb{C}_{\exp} is undecidable. Indeed, using the kernel of the exponential map, one can define the structure $(\mathbb{Z}, +, \cdot, 0, 1)$ inside \mathbb{C}_{\exp} . On the other side, the decidability problem for the theory of \mathbb{R}_{\exp} remains open. In [4], A. Macintyre and A. Wilkie highlight the role of Schanuel's

conjecture in this problem. More precisely, they prove that if Schanuel's conjecture is true then the theory of \mathbb{R}_{exp} is decidable. The main result of this paper is along this line:

Main theorem. Assume that the p -adic version of Schanuel's conjecture is true. Then the theory of the p -adic exponential ring is decidable.

The outline of the proof is the same that in the real case: first we reduce the decidability of the full theory to the case of existential sentences. In the real case, it relies (among other things) on the effective model-completeness of the theory of the reals in the language of ordered fields with the restricted exponential function. In the p -adic case, it is not known if the theory of $\mathbb{Z}_{p,exp}$ is model-complete. So, we will use the expansion of language \mathcal{L}_{pEC} introduced in [1]. In this language the theory of \mathbb{Z}_p is effectively model-complete. We recall the definition of this language in the beginning of section 4. While this language introduces new functions, it is not so different from the language \mathcal{L}_{exp} from the point of view of the decision problem for existential sentences. Indeed, the new functions can be written as polynomial combination of exponentials in a suitable finite algebraic extension of \mathbb{Q}_p . Therefore, in section 3, we will show that one can solve the decision problem for the positive existential \mathcal{L}_{exp} -sentences. Then in section 4, we will see how one can adapt the arguments to a general existential \mathcal{L}_{pEC} -sentence.

Let ψ be an existential \mathcal{L}_{exp} -sentence. It is sufficient to find a procedure that will return true when ψ is true in \mathbb{Z}_p (and may runs forever when ψ is false as by effective model-completeness the negation of ψ is also an existential \mathcal{L}_{pEC} -sentence). An easy case is when ψ is a formula of the type

$$\exists x_1, \dots, x_n P_1(\bar{x}, E_p(\bar{x})) = \dots = P_n(\bar{x}, E_p(\bar{x})) = 0 \neq J(\bar{x})$$

where J denote the Jacobian of the system.

In the real case, one can check that such a system of n exponential equations with n variables has a solution in \mathbb{R} using Newton algorithm. In our case, we will use an analytic version of Hensel's lemma.

Theorem 1.1 (Analytic Hensel's lemma). *Let $f = (f_1, \dots, f_t)$ be a system of elements in $\mathbb{Z}_p\{X_1, \dots, X_t\}$. Let $J_f(\bar{X})$ denote the Jacobian matrix of the system. Assume that there is $\bar{a} \in \mathbb{Z}_p^t$ such that*

$$\det J_f(\bar{a}) \neq 0 \text{ and } v(f(\bar{a})) > 2v(\det J_f(\bar{a})) + r,$$

where r is any nonnegative integer. Then, there is a unique $\bar{b} \in \mathbb{Z}_p^n$ such that

$$v(\bar{b} - \bar{a}) > v(\det J_f(\bar{a})) + r \text{ and } f(\bar{b}) = 0.$$

Assume that the formula ψ is realised in \mathbb{Z}_p , one can check it using Hensel's lemma:

1. Let $\bar{k}_1, \bar{k}_2, \dots$ be an enumeration of \mathbb{Z}^n .
2. For all i , check if $\det J_f(\bar{k}_i) \neq 0$ and $v(f(\bar{k}_i)) > 2v(\det J_f(\bar{k}_i))$.
3. If this is the case for some i , stops the procedure: the formula ψ is satisfied in \mathbb{Z}_p^n by Hensel's lemma.

Let us remark that whenever the formula ψ is true, we can always find such a tuple \bar{k}_i as \mathbb{Z}^n is dense in \mathbb{Z}_p^n .

We will reduce the general case to a procedure of this kind. More precisely, let $F_P(\bar{x}) = P(\bar{X}, E_p(\bar{x}))$ be an exponential polynomial with coefficients in \mathbb{Z} . Assume that the formula $\exists \bar{x} F_P(\bar{x}) = 0$ is realised in \mathbb{Z}_p . Then in section 2, we will prove a desingularization theorem i.e. that there are exponential polynomials $P_1(\bar{x}, E_p(\bar{x})), \dots, P_n(\bar{x}, E_p(\bar{x}))$ and a non-singular solution of the system which also a zero of F_P . While checking that the system has a non-singular solution is easy, it is not obvious that the solution we find is indeed the zero of F_P given by the theorem. Furthermore, we don't know any effective procedure to compute $P_1(\bar{x}, E_p(\bar{x})) = \dots = P_n(\bar{x}, E_p(\bar{x}))$. This is where we need a p -adic version of Schanuel's conjecture. We will see in section 4 that if we assume the p -adic Schanuel's conjecture, we can actually assume that P is (roughly) in the ideal generated by P_1, \dots, P_n . This will allow us to overcome the issues mentioned and give a positive answer to the decision problem for existential \mathcal{L}_{pEC} -sentences.

Notations. Let K be a valued field. We denote its valuation ring by \mathcal{O}_K and its maximal ideal by \mathfrak{M}_K . We will denote the p -adic valuation by v . We will denote the set of nonzero elements of a ring A by A^* .

2 Desingularization theorem

Let F be a subset of $\mathbb{Z}_p\{\bar{X}\}$. Let \mathcal{L}_F be the language $(+, \cdot, 0, 1, P_n, f; n \in \mathbb{N}, f \in F)$ where P_n is a unary predicate interpreted in \mathbb{Z}_p by the set of n th powers. We assume that the set of \mathcal{L}_F -terms is closed under derivation. The example of our interest is the case where F is the set of trigonometric functions (in the sense of [1], we recall the definition later in this paper) and E_p .

In this section, we consider a system of equations $f = (f_1, \dots, f_n)$ where the f_i 's are \mathcal{L}_F -terms with m variables. Assuming that the above system has a solution in \mathbb{Z}_p , we want to show that there exists a system of \mathcal{L}_F -terms $g = (g_1, \dots, g_m)$ such that there is a non-singular zero of the system g which is also a zero of the system f . We will actually prove the result for all finite algebraic extensions of \mathbb{Q}_p . This result is the p -adic version of theorem 5.1 in [8]. We will work with Noetherian differential rings like in [8]. The outline of the proof is actually the same that in the real case.

Within this section, K will denote a finite algebraic extension of \mathbb{Q}_p . The implicit function theorem will play an important role in our proof. We state now this result in the p -adic context.

Let $f : U \times V \rightarrow K^m$ be an analytic map (where $U \times V$ is an open subset of $K^n \times K^m$). Let $A = Df(\bar{a}, \bar{b})$ be its differential at (\bar{a}, \bar{b}) . We set

$$A_x = \begin{pmatrix} \frac{\partial f_1}{\partial x_1}(\bar{a}, \bar{b}) & \dots & \frac{\partial f_1}{\partial x_n}(\bar{a}, \bar{b}) \\ \vdots & & \vdots \\ \frac{\partial f_m}{\partial x_1}(\bar{a}, \bar{b}) & \dots & \frac{\partial f_m}{\partial x_n}(\bar{a}, \bar{b}) \end{pmatrix} \text{ and } A_y = \begin{pmatrix} \frac{\partial f_1}{\partial y_1}(\bar{a}, \bar{b}) & \dots & \frac{\partial f_1}{\partial y_m}(\bar{a}, \bar{b}) \\ \vdots & & \vdots \\ \frac{\partial f_m}{\partial y_1}(\bar{a}, \bar{b}) & \dots & \frac{\partial f_m}{\partial y_m}(\bar{a}, \bar{b}) \end{pmatrix}$$

Theorem 2.1 (Implicit function theorem). *Let $f : U \times V \rightarrow K^m$ be an analytic map (where $U \times V$ is an open subset of $K^n \times K^m$) such that $f(\bar{a}, \bar{b}) = 0$ for some $(\bar{a}, \bar{b}) \in U \times V$. Let $A = Df(\bar{a}, \bar{b})$. Assume A_y invertible. Then, there*

exist $U_1 \subset U$ and $U_2 \subset V$, both open and containing \bar{a} and \bar{b} respectively, such that for all $\bar{x} \in U_1$ there is a unique $\bar{y} \in U_2$ with $f(\bar{x}, \bar{y}) = 0$.

Furthermore, the map g defined by $g(\bar{x}) = \bar{y}$ from U_1 to U_2 is analytic and satisfies $g(\bar{a}) = \bar{b}$, $f(\bar{x}, g(\bar{x})) = 0$ for all $\bar{x} \in U_1$ and $Dg(\bar{x}) = -A_y^{-1}A_x$.

Let us remark that if the function f and the open sets U, V are definable, then so is the function g . Indeed, we can assume that the U_i 's are open balls and the function g is determined by the relations $(\bar{x}, g(\bar{x})) \in U_1 \times U_2$ and $f(\bar{x}, g(\bar{x})) = 0$. Also, the derivatives of g are definable via the relation $Dg(\bar{x}) = -A_y^{-1}A_x$.

We are now given a system f_1, \dots, f_n of \mathcal{L}_F -terms. We first observe that such a system can be reduced to a single equation in K : indeed, as $v(\mathcal{O}_K) = \frac{1}{e}\mathbb{Z}$ for some $e \in \mathbb{N}$:

$$\text{for all } x, y \in K, (x, y) = (0, 0) \text{ iff } x^2 + \pi y^2 = 0,$$

where π is an element of minimal positive valuation. So, we can consider systems with a single \mathcal{L}_F -term. We view K as a \mathcal{L}_F -structure (where $f \in F$ is interpreted by the map restricted to the valuation ring, i.e. the interpretation of f takes value $f(x)$ for $x \in \mathcal{O}_K$ and value 0 for $x \notin \mathcal{O}_K$). We also add to the language \mathcal{L}_F constant symbols for a basis of K over \mathbb{Q}_p (such that this basis is also a basis of \mathcal{O}_K over \mathbb{Z}_p). We are interested by the local behaviour of the definable analytic maps (especially, in what happens in the valuation ring). We consider the ring of such maps where we identify two maps which coincide on an open set i.e. the ring of germs:

Definition 2.2. Given a neighbourhood system \mathcal{N} in K^n (i.e. a non-empty collection of non-empty open \mathcal{L}_F -definable subsets of K^n closed under finite intersection), $\mathfrak{G}^{(n)}(\mathcal{N})^-$ is the set of all $\langle f, U \rangle$ where $U \in \mathcal{N}$ and $f : U \rightarrow K$ is a \mathcal{L}_F -definable function such that f is analytic on U .

We define an equivalence relation on $\mathfrak{G}^{(n)}(\mathcal{N})^-$ by: $\langle f_1, U_1 \rangle \sim \langle f_2, U_2 \rangle$ iff f_1 and f_2 coincide on a neighbourhood i.e. there is $U \in \mathcal{N}$ such that $U \subseteq U_1 \cap U_2$ and for all $x \in U$, $f_1(x) = f_2(x)$. We denote by $[f, U]$ the class of $\langle f, U \rangle$.

The ring of germs is the set $\mathfrak{G}^{(n)}(\mathcal{N}) = \mathfrak{G}^{(n)}(\mathcal{N})^- / \sim$ equipped with the natural operations of addition and multiplication.

Let us remark that $\mathfrak{G}^{(n)}(\mathcal{N})$ is a unital differential ring.

As a special case of neighbourhood system, we have the collection of all definable open neighbourhoods of a point P . We denote the ring of germs in this case by $\mathfrak{G}^{(n)}(P)$. Let $P \in K^l$ and $Q \in K^m$ and let f_1, \dots, f_m be analytic maps in $\mathfrak{G}^{(l+m)}(P, Q)$. Let $f = (f_1, \dots, f_m)$. Assume that $f(P, Q) = 0$ and $\det J_f(P, Q) \neq 0$ i.e. $f_i(P, Q) = 0$ for all i and

$$\det \begin{pmatrix} \frac{\partial f_1}{\partial x_{l+1}}(P, Q) & \dots & \frac{\partial f_1}{\partial x_{l+m}}(P, Q) \\ \vdots & & \vdots \\ \frac{\partial f_m}{\partial x_{l+1}}(P, Q) & \dots & \frac{\partial f_m}{\partial x_{l+m}}(P, Q) \end{pmatrix} \neq 0,$$

i.e. $f_i(P, Q) = 0$ for all i and the vectors

$$\left(\frac{\partial f_1}{\partial x_{l+1}}(P, Q), \dots, \frac{\partial f_1}{\partial x_{l+m}}(P, Q) \right), \dots, \left(\frac{\partial f_m}{\partial x_{l+1}}(P, Q), \dots, \frac{\partial f_m}{\partial x_{l+m}}(P, Q) \right)$$

are K -linearly independent. We denote these vectors by $d_{P,Q}f_i$. By the analytic implicit function theorem, there are $U_P \times U_Q \subset U$ and $\Phi' = (\Phi_{l+1}, \dots, \Phi_{l+m})$ analytic from U_P to U_Q such that $f_i(\bar{x}, \Phi_{l+1}(\bar{x}), \dots, \Phi_{l+m}(\bar{x})) = 0$ for all $\bar{x} \in U_P$. As the f_i 's and U are definable, this guarantees that the map Φ' is definable analytic. Therefore, Φ' determines a germ in $\mathfrak{G}^{(l)}(P)$.

Let $\Phi(\bar{x}) = (\Phi_1(\bar{x}), \dots, \Phi_{l+m}(\bar{x}))$ where $\Phi_i(\bar{x}) = x_i$ for $i \leq l$ and Φ_{l+i} as above. We denote the morphism of rings

$$\begin{aligned} \mathfrak{G}^{(l+m)}(P, Q) &\longrightarrow \mathfrak{G}^{(l)}(P) \\ [f, U] &\longmapsto [f(\Phi), U] \end{aligned}$$

by $\widehat{}$. The kernel of this map is the set of germs which vanish (locally) on the set of zeros of the system (f_1, \dots, f_m) around (P, Q) . In particular, $\hat{f}_i \equiv 0$ (and therefore, $\frac{\partial \hat{f}_i}{\partial x_j} \equiv 0$) in $\mathfrak{G}^{(l)}(P)$.

Lemma 2.3. *Let $f_1, \dots, f_m, (P, Q)$ as above. For all $g \in \mathfrak{G}^{(l+m)}(P, Q)$, $d_{P,Q}f_1, \dots, d_{P,Q}f_m, d_{P,Q}g$ are linearly independent over K iff $d_P \hat{g} \neq 0$.*

The proof of this lemma is word to word the same that lemma 4.7 in [8]. We fix now some notations: let $f_1, \dots, f_m : U \rightarrow K$ be analytic functions (where $U \subset K^n$ open). Then,

$$\begin{aligned} V(f_1, \dots, f_m) &= \{P \in U \mid f_1(P) = \dots = f_m(P) = 0\}, \\ V^{ns}(f_1, \dots, f_m) &= \{P \in V(f_1, \dots, f_m) \mid d_P f_1, \dots, d_P f_m \text{ are } K\text{-linearly independent}\}. \end{aligned}$$

Proposition 2.4. *Let $P \in K^n$ and let M be a Noetherian subring of $\mathfrak{G}^{(n)}(P)$ closed under differentiation. Let $m \in \mathbb{N}$ and $[f_1, U_1], \dots, [f_m, U_m] \in M$. Assume $P \in V^{ns}(f_1, \dots, f_m)$. Then, exactly one of the following is true:*

- (a) $n=m$; or,
- (b) $m < n$ and for all $[h, W] \in M$ with $h(P) = 0$, h vanishes on $U \cap V^{ns}(f_1, \dots, f_m)$ for some U open neighbourhood of P ; or,
- (c) $m < n$ and for some $[h, W] \in M$, $P \in V^{ns}(f_1, \dots, f_m, h)$.

Again the proof is similar to the real case [8]. Note that for this proposition, we need to consider analytic functions in our case (instead of infinitely differentiable functions in [8]).

Proof. If $m < n$, say $n = l + m$, then the vectors $d_P f_1, \dots, d_P f_m$ are linearly independent. Without loss of generality, we will assume that the matrix $A(P) = \left(\frac{\partial f_i}{\partial x_j}(P) \right)_{1 \leq i \leq m, l+1 \leq j \leq n}$ is invertible. Let λ be the map $\bar{x} \mapsto \det A(\bar{x})$. On a neighbourhood U of P , this map is invertible. Let $\Lambda = [\lambda, U]$. We define $M^* := M[\Lambda^{-1}]$. Assume $P = (P_1, P_2) \in K^{l \times m}$. We define the $\widehat{}$ -map as before. Then, $\widehat{M^*}$, the image of M^* by this map, is Noetherian. And, by the implicit function theorem, we have

$$\begin{pmatrix} \frac{\partial \Phi_{l+1}}{\partial x_r} \\ \vdots \\ \frac{\partial \Phi_n}{\partial x_r} \end{pmatrix} = -\Lambda^{-1} \begin{pmatrix} \frac{\partial f_1}{\partial x_r} \\ \vdots \\ \frac{\partial f_m}{\partial x_r} \end{pmatrix},$$

which means that $\frac{\partial \Phi_i}{\partial x_j} \in M^*$. Therefore using the chain rule, we find that $\widehat{M^*}$ is closed under differentiation.

Let $I = \{g \in \widehat{M^*} \mid g(P_1) = 0\}$.

1. If $I = \{0\}$. Suppose $g = [h, W] \in M$ and $h(P) = 0$. Then, $\hat{g}(P_1) = 0$ and therefore $\hat{g} \in I$ i.e. $\hat{g} = 0$. By definition of the map $\widehat{}$, it exactly means that h is vanishing on a neighbourhood of P in $V^{ns}(f_1, \dots, f_m)$.
2. If $I \neq \{0\}$, I is not closed under differentiation. Otherwise for all $g \in I$, the partial derivatives of g vanish at P_1 . This implies that all the coefficients of the power series defining g around P are zero and therefore $g = 0$ in $\widehat{M^*}$. So, there is $g \in M^*$ such that $\hat{g} \in I$ and $\frac{\partial \hat{g}}{\partial x_i} \notin I$. It means that $\hat{g}(P_1) = 0$ (i.e. $g(P) = 0$) and $\frac{\partial \hat{g}}{\partial x_i}(P_1) \neq 0$. But, for some integer s , $\Lambda^s g \in M$. Let $f = \Lambda^s g$. Then, $f(P) = 0$ and

$$\frac{\partial \hat{f}}{\partial x_i}(P_1) = \left(s \hat{\Lambda}^{s-1}(P_1) \frac{\partial \hat{\Lambda}}{\partial x_i} \hat{g}(P_1) \right) + \left(\hat{\Lambda}^s(P_1) \frac{\partial \hat{g}}{\partial x_i}(P_1) \right) \neq 0.$$

So, $d_P \hat{f} \neq 0$ and therefore by lemma 2.3, $P \in V^{ns}(f_1, \dots, f_m, f)$.

□

We are now able to state the desingularization theorem:

Let U be an open definable neighbourhood of the origin contained in \mathcal{O}_K^n . Then, $\{U\}$ forms a neighbourhood system. We denote the correspondent ring of germs by $\mathfrak{G}^{(n)}(U)$. Let us recall that we may assume $K = \mathbb{Q}_p(\alpha_1, \dots, \alpha_s)$ and that for this choice of $\alpha_1, \dots, \alpha_s$, $\mathbb{Z}(\alpha_1, \dots, \alpha_s)$ is dense in the valuation ring of K .

Theorem 2.5. *Let M be a Noetherian subring of $\mathfrak{G}^{(n)}(U)$ which contains $\mathbb{Z}(\overline{\alpha})[x_1, \dots, x_n]$, is closed under differentiation and such that for all $g \in M$, the germ of g is equivalent to a definable analytic function given by a power series with coefficients in the valuation ring.*

Let $f \in M$. Assume that S is a non-empty definable subset of $V(f)$, open in $V(f)$. Then, there exist $f_1, \dots, f_n \in M$ such that $S \cap V^{ns}(f_1, \dots, f_n) \neq \emptyset$.

Proof. First, for all $Q \in S$, we set $I_Q = \{g \in M \mid g(Q) = 0\}$. As M is Noetherian, there is some R in S such that I_R is maximal within the collection of all I_Q . Let g_1, \dots, g_N be generators of I_R and $g = \sum_i \pi^{2(i-1)} g_i^2$ (where π is a prime element of K which can be assumed to be one of the α_i). So, $g(x) = 0$ iff $g_i(x) = 0$ for all i . Then, $R \in V(g) \cap S$ and for all $Q \in V(g) \cap S$, $I_R = I_Q$. Choose m maximal such that for some $f_1, \dots, f_m \in M$, $R \in V^{ns}(f_1, \dots, f_m)$.

By contradiction, assume that $m < n$; say $n = m + l$.

Note that up to a $\mathbb{Z}(\overline{\alpha})$ -linear change of variables, we may assume R as close to the origin as we will need (more precisely, we need that the neighbourhood W_R below contains the origin). First, we will now prove that $V(g) \cap S$ and $V^{ns}(f_1, \dots, f_m)$ locally coincide.

(a) $V(g) \cap S \subseteq V^{ns}(f_1, \dots, f_m)$:

Indeed, $R \in V^{ns}(f_1, \dots, f_m)$. So, $f_i \in I_R$ for all i and $\det E \notin I_R$ (where E denotes the matrix $\left(\frac{\partial f_i}{\partial x_j} \right)$ with K -linearly independent vectors). As, for all $Q \in V(g) \cap S$, $I_Q = I_R$, it means that $f_i \in I_Q$ and $\det E \notin I_Q$. So, $Q \in V^{ns}(f_1, \dots, f_m)$.

(b) Let $Q \in V(g) \cap S$, $h \in M$ then $Q \notin V^{ns}(f_1, \dots, f_m, h)$:

If we assume $Q \in V^{ns}(f_1, \dots, f_m, h)$, arguing like in (a), we would find $R \in V^{ns}(f_1, \dots, f_m, h)$ which contradicts the maximality of m .

(c) For all $Q \in V(g) \cap S$, there is W_Q an open neighbourhood of Q such that $W_Q \cap V(g) \cap S = W_Q \cap V^{ns}(f_1, \dots, f_m)$:

By the point (b) and the proposition 2.4, the only possibility is that there is W' open neighbourhood of Q such that g vanishes on $W' \cap V^{ns}(f_1, \dots, f_m)$. As $f \in I_R$, it means that $V(f) \supseteq V(g)$ and therefore that f vanishes on $W' \cap V^{ns}(f_1, \dots, f_m)$. So, $W' \cap V^{ns}(f_1, \dots, f_m) \subseteq W' \cap V(g) \cap V(f)$. We have that S is open in $V(f)$. So, for some W'' open neighbourhood of Q , $W'' \cap S = W'' \cap V(f)$. Take $W_Q = W' \cap W''$ and we are done.

We are given f_1, \dots, f_m . Without loss of generality, we may assume that the matrix $\Delta = \left(\frac{\partial f_i}{\partial x_j} \right)_{1 \leq i \leq m; l+1 \leq j \leq n}$ has non-vanishing determinant at $R = (P, Q)$. Let $\Phi_{l+1}(\bar{x}), \dots, \Phi_n(\bar{x})$ given by the implicit function theorem and let $\Phi_i(\bar{x}) = x_i$ for $i \leq l$.

First, let us remark that up to a change of variables, we can assume that $\Phi_i(P)$ and $\frac{\partial \Phi_i}{\partial x_j}(P)$ (where $i > l \geq j$) lies in the maximal ideal \mathfrak{M}_K . Indeed, by a change of variables of the type $(X_1, \dots, X_n) \mapsto (X_1 - N_1, \dots, X_n - N_n)$ (where $N_i \in \mathbb{N}(\bar{\alpha})$ is a suitable approximation of P_i, Q_i), we can assume that the implicit functions are defined on a neighbourhood of 0. This means that we can assume $v(P) > t$ and $v(\Phi_i(P)) = v(Q) > t$ (where t could be any nonnegative integer). Also, we know that for all $r \leq l$

$$\begin{pmatrix} \frac{\partial \Phi_{l+1}}{\partial x_r} \\ \vdots \\ \frac{\partial \Phi_n}{\partial x_r} \end{pmatrix}(\bar{X}) = -\Delta^{-1} \begin{pmatrix} \frac{\partial f_1}{\partial x_r} \\ \vdots \\ \frac{\partial f_m}{\partial x_r} \end{pmatrix}(\bar{X}, \Phi_{l+1}(\bar{X}), \dots, \Phi_n(\bar{X})). \quad (1)$$

We consider the change of variables

$$(X_1, \dots, X_l, X_{l+1}, \dots, X_n) \mapsto (X_1, \dots, X_l, X_{l+1}/\pi^t, \dots, X_n/\pi^t).$$

Denote by \tilde{f} the function obtained after this change of variables. Then, for all $i \leq m$,

$$\frac{\partial \tilde{f}_i}{\partial x_j}(\tilde{P}, \tilde{Q}) = \begin{cases} \frac{\partial f_i}{\partial x_j}(P, Q) & \text{for } j \leq l \\ \pi^{-t} \frac{\partial f_i}{\partial x_j}(P, Q) & \text{for } l+1 \leq j \leq n, \end{cases}$$

where $(\tilde{P}, \tilde{Q}) = (P, \pi^t Q)$. So, $\tilde{\Delta}(\tilde{P}, \tilde{Q}) = \frac{1}{\pi^t} \Delta(P, Q)$. For t large enough, $\tilde{\Delta}(\tilde{P}, \tilde{Q})$ has negative valuation. Therefore, by the relation (1),

$$v \left(\frac{\partial \tilde{\Phi}_i}{\partial x_j}(\tilde{P}, \tilde{Q}) \right) > 0.$$

Without loss of generality, we will assume that such a changement has be done and will denote (\tilde{P}, \tilde{Q}) by (P, Q) and similarly for the functions.

Let $h_N(\bar{X}) := \sum (X_i - N_i)^2$ for all $N = (N_1, \dots, N_n) \in \mathbb{Z}[\alpha_1, \dots, \alpha_s]^n$. We want to apply Hensel's lemma to the functions $\left(\frac{\partial h_N}{\partial X_1}, \dots, \frac{\partial h_N}{\partial X_l} \right)$. Our goal

is to prove that for a point (P', Q') , close enough from (P, Q) , the vectors $d_{(P', Q')}f_1, \dots, d_{(P', Q')}f_m, d_{(P', Q')}h_N$ are linearly dependent. For this, by lemma 2.3, it is sufficient to check that the above partial derivatives vanish at P' .

We want to prove that if we choose N carefully, for all i , $\frac{\partial \hat{h}_N}{\partial X_i}(P)$ has valuation at least $2v(\det J(P)) + \varepsilon + 1$ where J is the Jacobian of the system, ε is the radius of the open set W_R given in (c). Then, the analytic Hensel's lemma gives us a root P' , ε -close from P .

Claim 1. $\det J(P) \neq 0$.

Proof. We compute the following derivatives using the chain rule :

$$g_i := \frac{\partial \hat{h}_N}{\partial X_i}(P) = \sum_{1 \leq k \leq n} 2 \cdot (\Phi_k(P) - N_k) \frac{\partial \Phi_k}{\partial X_i}(P).$$

$$\frac{\partial g_i}{\partial X_j}(P) = \frac{\partial^2 \hat{h}_N}{\partial X_j \partial X_i}(P) = \sum_k 2 \cdot \left(\frac{\partial \Phi_k}{\partial X_i}(P) \cdot \frac{\partial \Phi_k}{\partial X_j}(P) \right) + 2 \cdot (\Phi_k(P) - N_k) \frac{\partial^2 \Phi_k}{\partial X_j \partial X_i}(P).$$

We want to prove that the Jacobian of $g = (g_1, \dots, g_n)$ is non vanishing at P . In the above sum, let us denote $\sum_k 2 \cdot \frac{\partial \Phi_k}{\partial X_i}(P) \cdot \frac{\partial \Phi_k}{\partial X_j}(P)$ by B_{ij} and the other terms $\sum_k 2 \cdot (\Phi_k(P) - N_k) \frac{\partial^2 \Phi_k}{\partial X_j \partial X_i}(P)$ by C_{ij} . Then, let S_l be the permutation group of $\{1, \dots, l\}$ and $\text{sgn}(\sigma)$ be the signature of an element $\sigma \in S_l$. We have:

$$\begin{aligned} \det J_g(P) &= \sum_{\sigma \in S_l} \text{sgn}(\sigma) \prod J_{i\sigma(i)} \\ &= \sum \text{sgn}(\sigma) \prod (B_{i\sigma(i)} + C_{i\sigma(i)}) \\ &= \det B + (\dots), \end{aligned}$$

where in the sum (\dots) , each element contains at least one factor of the form $(\Phi_k(P) - N_k)$.

If $\det B \neq 0$, then, for N_k a suitable approximation of $\Phi_k(P)$, the valuation of $\det J_g(P)$ is given by the valuation of $\det B$ (let us remark that in this case this valuation does not depend on N). And therefore, $\det J_g(P) \neq 0$.

We remark that for all $k \leq l$, $\frac{\partial \Phi_k}{\partial X_i} \cdot \frac{\partial \Phi_k}{\partial X_j} = \delta_{ijk}$ (δ is the Kronecker delta). So, if we denote by D_{ij} the sum over $k > l$ in $B_{ij}/2$, we have: $\frac{1}{2}B = Id + D$ and

$$\begin{aligned} \frac{1}{2} \det B &= \sum_{\sigma \in S_r} \text{sgn}(\sigma) \cdot \prod (\delta_{i\sigma(i)} + D_{i\sigma(i)}) \\ &= (\det D - \prod D_{ii}) + \prod (1 + D_{ii}). \end{aligned}$$

Now, assume by contradiction that $\det B = 0$. Let us recall that for all $i > l$, for all k ,

$$v\left(\frac{\partial \Phi_i}{\partial X_k}(P)\right) > 0 \quad (*).$$

Therefore, $v(D_{ii}) > 0$ and as $\det B = 0$,

$$v\left(\det D - \prod D_{ii}\right) = v\left(\prod (1 + D_{ii})\right) = 0.$$

We deduce from these relations that $v(\det D) = 0$. This is a contradiction with (*).

This completes the proof of the claim. \square

Now, for $N_k \in \mathbb{Z}[\alpha_1, \dots, \alpha_s]$ a suitable approximation of $\Phi_k(P)$, $g_i(P)$ has valuation at least $2v(\det J(P)) + \varepsilon + 1$ (as we have seen the valuation of $J(P)$ does not depend on N in this case). So, by Hensel's lemma, there exists P' (ε -close from P) such that for all i , $g_i(P') = 0$ i.e. $d_{P'} h_N = 0$.

Let $Q' = (\Phi_{l+1}(P'), \dots, \Phi_n(P'))$. Then, $(P', Q') \in V^{ns}(f_1, \dots, f_m)$ and by lemma 2.3, $d_{(P', Q')} f_1, \dots, d_{(P', Q')} f_m, d_{(P', Q')} h_N$ are linearly dependent over K . But, as (P', Q') is in W_R (if we pick ε small enough), we have that $(P', Q') \in V^{ns}(f_1, \dots, f_m) \cap W_R \subseteq V(g) \cap S$. Then, by an argument similar to the proof of (a), $d_{(P, Q)} f_1, \dots, d_{(P, Q)} f_m, d_{(P, Q)} h_N$ are also linearly dependent for all N suitable approximation of $\Phi(P)$. As $d_{(P, Q)} f_1, \dots, d_{(P, Q)} f_m$ are linearly independent, it implies that $d_{(P, Q)} h_N$ lies in the linear span of the other vectors.

Let $N' = (N_1, \dots, N_{i-1}, N_i + p^{t_i}, N_{i+1}, \dots, N_n)$, then N' is also a suitable approximation of $\Phi(P)$ (for all t_i large enough) and therefore $d_{(P, Q)} h_{N'}$ lies in the same vector space. But then, $(0, \dots, p^{t_i}, 0, \dots, 0) = (d_{(P, Q)} h_{N'} - d_{(P, Q)} h_N)/2$ lies in the linear span of $d_{(P, Q)} f_1, \dots, d_{(P, Q)} f_m$ for all i , which contradicts that $m < n$. \square

Our desingularization result is an immediate corollary of this theorem:

Corollary 2.6. *Let $F \subset \mathcal{O}_K\{\overline{X}\}$. Assume that the set of \mathcal{L}_F -terms is closed under derivation and that for any finite collection of \mathcal{L}_F -terms, the ring generated by these terms, their subterms and their derivatives is Noetherian. Let f be a \mathcal{L}_F -term and assume that the formula $\exists x_1 \dots \exists x_n f(\overline{x}) = 0$ is satisfied in \mathcal{O}_K . Then there are f_1, \dots, f_n \mathcal{L}_F -terms such that the formula*

$$\exists \overline{x} f(\overline{x}) = f_1(\overline{x}) = \dots = f_n(\overline{x}) = 0 \neq \det J_{(f_1, \dots, f_n)}(\overline{x})$$

is satisfied in \mathcal{O}_K .

Proof. Let f be a \mathcal{L}_F -term. Then, we apply the theorem 2.5 with $U = \mathcal{O}_K$, M the ring generated over $\mathbb{Z}(\overline{\alpha})$ by the subterms of f and their derivatives. We take $S = V(f)$. The theorem exactly says that if $V(f) \neq \emptyset$, then there are $f_1, \dots, f_n \in M$ and $\overline{\alpha} \in \mathcal{O}_K^n$ such that

$$f(\overline{\alpha}) = f_1(\overline{\alpha}) = \dots = f_n(\overline{\alpha}) = 0 \neq \det J_{(f_1, \dots, f_n)}(\overline{\alpha}).$$

Finally, let us remark that as the set of \mathcal{L}_F -terms is closed under derivation, any element of M is a \mathcal{L}_F -term. \square

Corollary 2.7. *Let $P(X_1, \dots, X_n, Y_1, \dots, Y_n) \in \mathbb{Z}[\overline{X}, \overline{Y}]$. Assume that $f(X) = P(\overline{X}, E_p(\overline{X}))$ has a root in \mathbb{Z}_p . Then there is $P_1, \dots, P_n \in \mathbb{Z}[\overline{X}, \overline{Y}]$ and $\overline{b} \in \mathbb{Z}_p^n$ such that*

$$P(\overline{b}, E_p(\overline{b})) = P_1(\overline{b}, E_p(\overline{b})) = \dots = P_n(\overline{b}, E_p(\overline{b})) = 0 \neq \det J_{(P_1, \dots, P_n)}(\overline{b}).$$

Proof. Apply theorem 2.5 with $U = \mathbb{Z}_p$, $M = \mathbb{Z}[\overline{X}, E_p(\overline{X})]$ and $S = V(P(\overline{X}, E_p(\overline{X})))$. \square

3 Decidability of positive existential sentences

It is easy to see that any existential \mathcal{L}_{exp} -sentence is (effectively) equivalent to a disjunction of sentences of the type:

$$\exists x_1 \cdots \exists x_n \bigwedge_j F_j(\bar{x}) = 0 \wedge \bigwedge_j G_j(\bar{x}) \neq 0,$$

where F_i and G_j are in $\mathbb{Z}[x_1, \dots, x_n, e^{p^{x_1}}, \dots, e^{p^{x_n}}]$. Note that unlike the real case, we cannot remove the inequalities (in the real case, we can remove inequality at the price of new variables because nonzero elements are invertible).

Let us remark that to any such exponential polynomial F corresponds a polynomial in $\mathbb{Z}[x_1, \dots, x_{2n}]$. And conversely, to a polynomial $P \in \mathbb{Z}[x_1, \dots, x_{2n}]$ corresponds a unique element of $\mathbb{Z}[x_1, \dots, x_n, e^{p^{x_1}}, \dots, e^{p^{x_n}}]$. We will denote by F_P this exponential polynomial.

We start with the case where only equalities are involved. Once again, as for all $x, y \in \mathbb{Z}_p$ $(x, y) = (0, 0)$ iff $x^2 + py^2 = 0$, we are reduced to the case of a single exponential polynomial, say $F_P(x_1, \dots, x_n)$. First, note that it is not hard to check that a given positive existential sentence is false in \mathbb{Z}_p :

Lemma 3.1. *Let $U = \bar{a} + p^t \mathbb{Z}_p^n$ be an open set (where $\bar{a} \in \mathbb{Z}^n$, $t \in \mathbb{N}$) and let $g = (g_1, \dots, g_k)$ be k exponential functions. Then, there is a recursive procedure which returns yes if there is no zero of g inside U .*

Proof. We just have to check that the valuation of g is bounded on U .

Let us remark that if there is $\bar{y} \in U$ such that $g(\bar{y}) = 0$, then for all $s \geq t$, there are $b_{0i}, \dots, b_{si} \in \{0, \dots, p-1\}$, $i \leq n$ such that

$$a_i \equiv \sum_j b_{ji} p^j \pmod{p^t} \text{ and } g\left(\sum_j b_{j1} p^j, \dots, \sum_j b_{jk} p^j\right) \equiv 0 \pmod{p^{s+1}}.$$

Actually, the b_{ji} 's are the digits of b_i a suitable approximation of y_i .

So, the converse states that: if there is $s \geq t$ such that for all $b_{0i}, \dots, b_{si} \in \{0, \dots, p-1\}$ such that for all $i \leq n$

$$a_i \equiv \sum_j b_{ji} p^j \pmod{p^t},$$

we have

$$g\left(\sum_j b_{j1} p^j, \dots, \sum_j b_{jk} p^j\right) \not\equiv 0 \pmod{p^{s+1}},$$

then, there is no $\bar{y} \in U$ such that $g(\bar{y}) = 0$.

But these last conditions are recursively enumerable. The following algorithm does the job:

Algorithm 1. *Given $U = \bar{a} + p^t \mathbb{Z}_p^n$, $g = (g_1, \dots, g_k)$.*

Proceed to an enumeration of all $s \in \mathbb{N}$, $s \geq t$. Check if for all $b_1, \dots, b_n \in \mathbb{Z}/p^s \mathbb{Z}$ with $v(\bar{a} - \bar{b}) \geq t$, $g_i(\bar{b}) \not\equiv 0 \pmod{p^{s+1}}$ for all i . If yes, return true. Otherwise go to the next step.

This completes the proof of the lemma. \square

Let us remark that this algorithm never stops if the system has a root in U . Note that we are able to do the basic computations in the above lemma (and in the rest of the paper) effectively. Indeed, we are able to compute the valuation of an exponential polynomial evaluated at a given integer.

Let $f \in \mathbb{Z}[x_1, \dots, x_n, e^{px_1}, \dots, e^{px_n}]$ and a tuple of integer \bar{t} . Then, we are able to determine if $f(\bar{t}) = 0$ and compute the valuation of $f(\bar{t})$: Let us remark that we can assume that $f(\bar{t})$ is a finite sum of the form

$$f(\bar{t}) = s \sum a_i e^{p_i}$$

where the a_i 's are integer and $s \in \mathbb{Z}_p^*$. As, e^p is transcendental over \mathbb{Q} (theorem due to Malher [5]), $f(\bar{t}) = 0$ iff $a_i = 0$ for all i . If this is not the case, using the Taylor expansion, we can determine the remainder of $f(\bar{t})$ modulo p^n for all n . The valuation of $f(\bar{t})$ is determined by the smallest n such that $f(\bar{t}) \not\equiv 0 \pmod{p^n}$.

Let $\psi \equiv \exists \bar{x} F_P(\bar{x}) = 0$ be a positive existential formula. The above lemma gives us a procedure which stops and returns true if ψ is false in \mathbb{Z}_p . It runs forever if ψ is true in \mathbb{Z}_p . To complete the proof of the decidability of the set of positive existential formula, we just have to give a procedure that returns true whenever F_P has a root in \mathbb{Z}_p (and may runs forever otherwise). Actually, using the desingularization theorem, we can almost already determine if F_P has a root in \mathbb{Z}_p :

Assume that F_P admits a root \bar{a} in \mathbb{Z}_p^n , then we know by the corollary 2.7 that there are F_{P_1}, \dots, F_{P_n} and \bar{b} such that $F_P(\bar{b}) = 0$ and \bar{b} is a non-singular zero of the system $G = (F_{P_1}, \dots, F_{P_n})$. Now, by Hensel's lemma, we can check if the system G has a non-singular solution in \mathbb{Z}_p . However, there is two issues: first, the system G is not given explicitly in the proof of the desingularization theorem (i.e. may not be computable). Second, there is no guarantee that the non-singular solution of the system G computed by Hensel's lemma is indeed a solution of F_P .

The two issues can be solved if P is in the ideal generated by P_1, \dots, P_n . Indeed, in that case, \bar{b} determines a zero of each P_i :

$$P_i(b_1, \dots, b_n, e^{pb_1}, \dots, e^{pb_n}) = 0 \text{ iff } F_{P_i}(b_1, \dots, b_n) = 0.$$

And conversely, any zero $b_1, \dots, b_n, e^{pb_1}, \dots, e^{pb_n}$ of the system P_1, \dots, P_n is a zero of P . Furthermore, we can find P_1, \dots, P_n by enumerating all polynomials in $\mathbb{Z}[\bar{X}]$ (see later for more details).

The next lemma will give us exactly what we need : up to multiplication by a polynomial Q (such that Q does not vanish at $(b_1, \dots, b_n, e^{pb_1}, \dots, e^{pb_n})$), P is in the ideal generated by some Q_1, \dots, Q_n like above. The key point of this lemma is that we can determine the transcendence degree of $\mathbb{Q}(b_1, \dots, b_n, e^{pb_1}, \dots, e^{pb_n})$ over \mathbb{Q} . This is where Schanuel's conjecture turns out to be helpful.

The first thing to observe is that as \bar{b} is a non-singular zero of the system G , we certainly have that

$$\text{trdeg}_{\mathbb{Q}} \mathbb{Q}(b_1, \dots, b_n, e^{pb_1}, \dots, e^{pb_n}) \leq n.$$

We will actually need equality which can be obtained using a p -adic version of Schanuel's conjecture:

Conjecture (*p*-adic Schanuel's Conjecture). *Let $n \geq 1$ and t_1, \dots, t_n in \mathbb{C}_p (with valuation at least $1/(p-1)$) linearly independent over \mathbb{Q} .*

Then, the field $\mathbb{Q}(t_1, \dots, t_n, e^{t_1}, \dots, e^{t_n})$ has transcendence degree at least n over \mathbb{Q} .

Using the *p*-adic version of Schanuel's conjecture, like in [4], we can prove:

Lemma 3.2. *Let $n \geq 1$, $P \in \mathbb{Z}[x_1, \dots, x_{2n}]$.*

Assume that $F_P = P(x_1, \dots, x_n, e^{px_1}, \dots, e^{px_n})$ has a zero and that for all zeros \bar{a} of F_P , its components a_1, \dots, a_n are \mathbb{Q} -linearly independent.

Then, there exist $b_1, \dots, b_n \in \mathbb{Z}_p$ and $Q, Q_1, \dots, Q_n, S_1, \dots, S_n \in \mathbb{Z}[x_1, \dots, x_{2n}]$ such that \bar{b} is a zero of F_P and a non-singular zero of $G = (F_{Q_1}, \dots, F_{Q_n})$, that $F_Q(\bar{b}) \neq 0$ and that $QP = \sum_i Q_i S_i$.

This lemma guarantees the existence of a system such that the non-singular zeros of this system are roots of F_P .

Proof. Let P_1, \dots, P_n given by corollary 2.7 and $\bar{b} \in V(F_P) \cap V^{ns}(F_{P_1}, \dots, F_{P_n})$.

By the above discussion, the transcendence degree of $\mathbb{Q}(b_1, \dots, b_n, e^{pb_1}, \dots, e^{pb_n})$ over \mathbb{Q} is exactly n . We apply the following claim with $m = 2n$, $r = n$ and $I = \{h \in \mathbb{Z}[x_1, \dots, x_{2n}] \mid h(b_1, \dots, b_n, e^{pb_1}, \dots, e^{pb_n}) = 0\}$:

Claim 2. *Let $m, r \geq 1$, I prime ideal of $\mathbb{Z}[x_1, \dots, x_m]$ with $I \cap \mathbb{Z} = \{0\}$ and $\text{trdeg}_{\mathbb{Q}} \text{Frac}(\mathbb{Z}[x_1, \dots, x_m]/I) = r$. Then, there is $Q \in \mathbb{Z}[\bar{x}]$ with $Q \notin I$ such that QI is generated by $m - r$ elements.*

As $\text{trdeg} \text{Frac}(\mathbb{Z}[\bar{x}]/I) = \text{trdeg}_{\mathbb{Q}} \mathbb{Q}(b_1, \dots, b_n, E_p(b_1), \dots, E_p(b_n)) = n$ (by Schanuel's conjecture), we can apply the claim.

Let Q_1, \dots, Q_n be generators of QI . Then, the properties of the lemma are satisfied except that \bar{b} may be a singular zero of our system. But, as $P_i \in I$, $QP_i = \sum S_{ij} Q_j$ for some $S_{ij} \in \mathbb{Z}[\bar{x}]$. Using the chain rule on this relation, we find that

$$F_Q(\bar{b}) \cdot \frac{\partial F_{P_i}}{\partial x_j}(\bar{b}) = \sum_k F_{S_{ik}}(\bar{b}) \frac{\partial F_{Q_k}}{\partial x_j}(\bar{b}).$$

As $F_Q(\bar{b}) \neq 0$, we deduce that \bar{b} is a non-singular zero of G . \square

Proposition 3.3. *If Schanuel's conjecture is true, the positive existential theory of the structure $(\mathbb{Z}_p, +, \cdot, 0, 1, E_p)$ is decidable.*

Proof. Let φ be a positive existential sentence of our theory. Without loss of generality, we can assume that

$$\varphi \equiv \exists x_1 \dots x_n F_P(\bar{x}) = 0$$

for some $P \in \mathbb{Z}[X_1, \dots, X_{2n}]$.

First, we give an algorithm that returns true if the sentence is satisfied (and never stop otherwise). We are given F_P and we want to know if this function admits a solution in \mathbb{Z}_p^n . Assume that this is the case. Then, lemma 3.2 gives us the existence of exponential polynomial functions $G = (F_{Q_1}, \dots, F_{Q_n})$ such that any non-singular zero of G is a zero of F_P . So, proceed to an enumeration over all possible system G and polynomials Q, S_{ij} like in the lemma. Using Hensel's lemma, we can determine if G has a non-singular root in an open U . If our sentence is satisfied, there exists such an open set U which contains a solution

of G and does not contain a root of F_Q . So, we proceed to an enumeration of all open set of the type $U = \bar{a} + p^t \mathbb{Z}_p^n$ for all $\bar{a} \in \mathbb{N}^n, t \in \mathbb{N}$ and on each such a set we check if the conditions of Hensel's lemma are satisfied for some tuple in U and if F_Q has no root in U (via lemma 3.1).

We give now the algorithm. If Schanuel's conjecture is true, this algorithm returns true whenever F_P has at least one root in \mathbb{Z}_p^n and the components of any of its roots are linearly independent. If these conditions are not satisfied, this algorithm may run forever.

Algorithm 2. *Given $n \geq 1, P \in \mathbb{Z}[x_1, \dots, x_{2n}]$.*

Proceed to an enumeration of $Q, Q_1, \dots, Q_n, S_1, \dots, S_n \in \mathbb{Z}[x_1, \dots, x_{2n}]$ and all $a_1, \dots, a_n, t, s \in \mathbb{N}, s \geq t$

Given such a $3n+3$ -uple, first check if $QP = \sum Q_i S_i$. If not go to the next step (of the enumeration).

Otherwise, check if

$$\det \left(\frac{\partial F_{Q_i}}{\partial x_j} \right) (\bar{a}) \neq 0,$$

and if

$$v(F_{Q_i})(\bar{a}) > v \left(\det \left(\frac{\partial F_{Q_i}}{\partial x_j} \right) (\bar{a}) \right) + t.$$

If not, go to the next step.

If this is the case (there is a root of the system G in $U := \bar{a} + p^t \mathbb{Z}_p^n$), for all $b_{ij} \in \{0, \dots, p-1\}$, where $0 \leq j \leq s, 1 \leq i \leq n$, let $b_i = \sum b_{ij} p^j$ check if whenever $v(\bar{b} - \bar{a}) \geq t$, we have

$$F_Q(\bar{b}) \not\equiv 0 \pmod{p^{s+1}}.$$

If yes (F_Q does not admit root in U), return true. Otherwise, go to the next step.

Finally, let us recall that in the above algorithm, we need to assume that the components of any root of F_P are linearly independent. But, without loss of generality, we can assume that this is the case:

Indeed, let F_P be an exponential polynomial. We proceed to an enumeration over all possible relations of \mathbb{Z} -linear dependence between the variables and we run in parallel the following procedure:

For each relation, we remove one of the variable according to this relation. Let \widetilde{F}_P be the exponential polynomial obtained after this transformation. We remark that \widetilde{F}_P has a root iff F_P has a root that satisfies the \mathbb{Z} -linear relation used to construct \widetilde{F}_P . We apply the algorithm 2 with entry \widetilde{F}_P . If the components of any root of \widetilde{F}_P are linearly independent, then algorithm 2 returns true (in the case where \widetilde{F}_P has a root) and the truth of our formula is determined. If \widetilde{F}_P has a root with components linearly dependent, we restart the procedure with $F_P := \widetilde{F}_P$.

This procedure stops and returns true in the case where F_P has a root in \mathbb{Z}_p .

Now, we can determine the truth of a positive existential sentence : we run in parallel the algorithm 1 and algorithm 2 with entries P . If F_P has no root in \mathbb{Z}_p^n , the algorithm 1 stops and we return false. If not, then F_P has a root and algorithm 2 stops, in which case, we return true. \square

Remark. It is not hard to see that the algorithms 1 and 2 can be adapted to determine the truth of positive existential sentences in $(\mathcal{O}_K, +, \cdot, 0, 1, E_p)$ where K is a finite algebraic extension of \mathbb{Q}_p .

Let us also remark that the algorithm 2 can be easily modified to take as entries general existential sentences. Indeed, such a sentence has the form

$$\exists x_1 \cdots \exists x_n F_P(\bar{x}) = 0 \wedge \bigwedge_j F_{R_j}(\bar{x}) \neq 0.$$

Therefore, we just have to check that F_{R_j} has no root in U (exactly like we did for F_Q). However, it is not clear that we can find a procedure that stops if such a sentence is false. One could proof that the negation of the above formula is equivalent to a (computable) \mathcal{L}_{exp} -existential sentence. It is not known if such a model-completeness result exists. In order to avoid this issue, we extend proposition 3.3 to the expansion of language \mathcal{L}_{pEC} of [1]. In this language, the theory of \mathbb{Z}_p is effectively model-completene. The decidability of the full theory is then clear: apply the above procedure in parallel for the sentence and (the \mathcal{L}_{pEC} -existential sentence equivalent to) its negation. One of the two procedure has to stop and therefore determines the truth of the sentence in \mathbb{Z}_p .

4 Decidability of the \mathcal{L}_{pEC} -sentences

First, let us recall the definition of the language used in [1] to obtain the model-completeness result. Let $K = \mathbb{Q}_p(\alpha)$ be a finite algebraic extension of degree d (where we assume α has nonnegative valuation and is algebraic over \mathbb{Q}). We want to expand \mathcal{L}_{exp} by function symbols so that the function $E_p : \mathbb{Z}_p(\alpha) \rightarrow \mathbb{Z}_p(\alpha)$ is definable in our language. As usual, one can define the ring $\mathbb{Z}_p(\alpha)$ in \mathbb{Z}_p by identifying the former ring with its structure of \mathbb{Z}_p -module. So, it is sufficient to be able to decompose $E_p(y)$ in the basis of K over \mathbb{Q}_p for all $y \in \mathbb{Z}_p(\alpha)$. By the multiplicative property of E_p we actually just need to decompose $E_p(x\alpha^i)$ for all $i < d$ and for all $x \in \mathbb{Z}_p$. We set

$$E_p(x\alpha^i) = c_{0,i}(x) + c_{1,i}(x)\alpha + \cdots + c_{d-1,i}(x)\alpha^{d-1}.$$

The elements $c_{i,j}(x)$ define functions from $\mathbb{Z}_p \rightarrow \mathbb{Z}_p$ such that $c_{i,j}(X) \in \mathbb{Z}_p\{X\}$. We call these functions the *decomposition functions of E_p in K* . Note that these functions does not depend on the choice of the basis. Indeed, let $\sigma \in \text{Gal}(K/\mathbb{Q}_p)$ (the Galois group of K over \mathbb{Q}_p) then

$$E_p(x\sigma(\alpha)^i) = c_{0,i}(x) + c_{1,i}(x)\sigma(\alpha) + \cdots + c_{d-1,i}(x)\sigma(\alpha)^{d-1}.$$

In fact, just like the function \sin and \cos in \mathbb{C} , the functions c_i can be expressed as a polynomial combination of $E_p(x\sigma(\alpha))$. Indeed, from the above equalities, we find that:

$$\begin{pmatrix} c_{0,i}(x) \\ \vdots \\ c_{d-1,i}(x) \end{pmatrix} = V^{-1} \begin{pmatrix} E_p(x\sigma_0(\alpha)) \\ \vdots \\ E_p(x\sigma_{d-1}(\alpha)) \end{pmatrix} (*),$$

where V is the Vandermonde matrix of the roots of the minimal polynomial of α and σ_i are the elements of $\text{Gal}(K_d/\mathbb{Q}_p)$.

We fix a tower of finite algebraic extensions $K_1 \subset K_2 \subset \cdots$ so that

- K_n is the splitting field of $Q_n(X)$ polynomial of degree N_n with coefficients in \mathbb{Q} ;
- $K_n = \mathbb{Q}_p(\beta_n)$ for all β_n root of Q_n ;
- any extension of degree n is contained in K_n and its valuation ring is contained in $\mathbb{Z}_p[\beta_n]$.

Note that by Krasner lemma, such a family of extension exists. We denote by c_{ijn} the decomposition functions of E_p in K_n . Let $\mathcal{L}_{pEC} = \mathcal{L}_{exp} \cup \{c_{ijn} : i < N_j, j, n \in \mathbb{N}\}$. We will say the functions c_{ijn} are the *trigonometric functions*.

Let \mathbb{Z}_{pEC} be the structure with underlying set \mathbb{Z}_p and natural interpretations for the language \mathcal{L}_{pEC} . In [7], it is proved that

Theorem 4.1. *Th(\mathbb{Z}_{pEC}) is effectively strongly model-complete.*

Therefore, if we are able to solve the decision problem for \mathcal{L}_{pEC} -existential sentences then the theory of $\mathbb{Z}_{p,exp}$ is decidable.

Let φ be an existential \mathcal{L}_{pEC} -sentence with n quantifiers. Then, there is N such that any term of the formula has the form

$$f(\bar{x}) = P(\bar{x}, e^{p\bar{x}}, c_{0,1,N}(\bar{x}), \dots, c_{d_N-1,d_N-1,N}(\bar{x})) =: F_P(\bar{x})$$

for some $P(\bar{x}, \bar{y}_0, \dots, \bar{y}_{L_N}) \in \mathbb{Z}[\bar{x}, \bar{y}_0, \dots, \bar{y}_{L_N}]$ (where $L_N = d_N^2 - d_N$). Let us remark that the ring generated by the exponential and trigonometric functions is closed under derivation. Therefore, we can apply theorem 2.5:

Let f be a \mathcal{L}_{pEC} -term. Assume that $V(f) \neq \emptyset$. Then, there exist $Q_1, \dots, Q_n \in \mathbb{Z}[\bar{x}, \bar{y}_0, \dots, \bar{y}_{L_N}]$ such that $V^{ns}(F_{Q_1}, \dots, F_{Q_n}) \cap V(f) \neq \emptyset$. This implies that there is a root \bar{a} of f such that:

$$\begin{aligned} \text{trdeg}_{\mathbb{Q}} \mathbb{Q}(a_1, \dots, a_n, e^{pa_1}, \dots, e^{pa_n}, c_{0,1,d_N}(a_1), \dots, c_{d_N-1,d_N-1,N}(a_n)) \\ = \text{trdeg}_{\mathbb{Q}} \mathbb{Q}(a_1, \dots, a_n, e^{pa_1}, \dots, e^{pa_n}, e^{pa_1\beta_N} \dots, e^{pa_n\beta_N^{d_N-1}}) \leq d_N \cdot n, \end{aligned}$$

where the first equality holds, as by (*), the trigonometric functions can be expressed as a polynomial combinations of $E_p(x\beta_N^k)$. Let us remark that $1, \beta_N, \dots, \beta_N^{d_N-1}$ are \mathbb{Q}_p -linearly independent. Using the p -adic Schanuel's conjecture, we find that the above relation is actually an equality (if a_1, \dots, a_n are \mathbb{Q} -linearly independent). With this, we prove as before:

Lemma 4.2. *Let $n \geq 1$, $P \in \mathbb{Z}[\bar{X}, \bar{Y}_0, \dots, \bar{Y}_{L_N}]$.*

Assume that $F_P = P(x_1, \dots, x_n, e^{px_1}, \dots, e^{px_n}, c_{0,1,N}(x_1), \dots, c_{d_N-1,d_N-1,N}(x_n))$ has a zero in \mathbb{Z}_p and that the components of any zero of F_P are \mathbb{Q} -linearly independent.

Then, there exist $a_1, \dots, a_n \in \mathbb{Z}_p$ and $R, R_1, \dots, R_{T_N}, S_1, \dots, S_{T_N} \in \mathbb{Z}[\bar{X}, \bar{Y}_0, \dots, \bar{Y}_{L_N}]$ (where $T_N = (L_N - d_N + 2) \cdot n$) such that \bar{a} is a zero of F_P and a non-singular zero of a subsystem of $G = (F_{R_1}, \dots, F_{R_{T_N}})$, that $F_R(\bar{a}) \neq 0$ and that $RP = \sum_i R_i S_i$.

Proof. We apply claim 2 with

$$I = \{h \in \mathbb{Z}[\bar{X}, \bar{Y}_0, \dots, \bar{Y}_{L_N}] \mid h(\bar{a}, E_p(\bar{a}), c_{0,1,N}(\bar{a}), \dots, c_{d_N-1,d_N-1,N}(\bar{a})) = 0\},$$

$m = (L_N^2 + 2) \cdot n$ and $r = d_N \cdot n$. Then, by the claim, there exist $R \notin I$, R_1, \dots, R_{T_N} generators of RI (where $T_N = m - r$) and S_1, \dots, S_{T_N} such that $RP = \sum R_i S_i$. Also, as $Q_i \in I$ for all i , like in lemma 3.2, it implies that $\bar{a} \in V^{ns}(F_{\widetilde{R_1}}, \dots, F_{\widetilde{R_n}})$ for some $\widetilde{R_1} \dots, \widetilde{R_n} \in \{R_1, \dots, R_{T_N}\}$. \square

If we are given φ an existential \mathcal{L}_{pEC} -sentence of the form:

$$\exists x_1, \dots, x_n F_P(\bar{x}) = 0 \wedge \bigwedge_i F_{A_i}(\bar{x}) \neq 0,$$

it is quite easy to adapt the algorithm 2 to construct an algorithm that returns yes if the sentence is true in \mathbb{Z}_p (and never stops otherwise):

1. Enumerate all $R, R_1, \dots, R_{T_N}, S_1, \dots, S_{T_N}$ and $B = \bar{a} + p^k \mathbb{Z}_p^n$.
2. If $RP = \sum R_i S_i$, check if a subsystem $\widetilde{R}_1 \dots, \widetilde{R}_n$ has a unique non-singular root in B using Hensel's lemma.
3. If this is the case, use the algorithm 2 to determine if the following formula is true in V_N :

$$\exists \bar{x} \bar{x} \in B \wedge \bar{x} \in V^{ns}(\widetilde{R}_1 \dots, \widetilde{R}_n) \wedge \bar{x} \in V(R_1, \dots, R_{T_N}).$$

We use the version of algorithm 2 for formulas in K_N and in the above formula, we replace the trigonometric functions by their polynomial expression in exponential terms. Note that this procedure never stops if the above formula is false but it doesn't matter.

4. If the above formula is true, then the system R_1, \dots, R_{T_N} has a root in $\mathbb{Z}_p^n \cap B$. So, F_P has a root in $\mathbb{Z}_p^n \cap B$. It remains to check that F_{A_i} and F_R have no root in B . If this is the case, φ is true.

Now, we use theorem 4.1 to obtain a sentence ψ equivalent to the negation of the sentence φ . Surely, our algorithm stops either for φ or ψ . We can therefore determine the truth value of φ in \mathbb{Z}_p by running in parallel the algorithm for φ and ψ .

The main theorem follows:

Theorem 4.3. *Assume that the p -adic version of Schanuel's conjecture is true. Then, the theory of \mathbb{Z}_{pEC} is decidable.*

Remark. • By the remark after proposition 3.3, it is not hard to extend the above theorem to finite algebraic extensions of \mathbb{Q}_p .

- In the above theorem, we actually use the p -adic Schanuel's conjecture for point in the algebraic closure of \mathbb{Q}_p (i.e. we don't need the case where the α_i 's are proper points of \mathbb{C}_p).
- For sentences in one variable, one can solve the decision problem unconditionally (see [6]).

References

- [1] A. Macintyre. The elementary theory of p -adic exponentiation. Unpublished notes.
- [2] A. Macintyre. Decision problems for exponential rings: the p -adic case. *Lecture Notes in Comput. Sci., Vol. 158*, pages 285–289, 1983.

- [3] A. Macintyre. Effective determination of the zeros of p -adic exponential functions. *Annals of Discrete Mathematics*, 24, pages 103–110, 1985.
- [4] A. Macintyre and A. Wilkie. On the decidability of the real exponential field. *Kreiseliana*, 441–467, A K Peters, Wellesley, pages 441–467, 1996.
- [5] K. Malher. Ein beweis der transzendenz der p -adischen exponentialfunktion. *J. Reine Angew. Math.*, Issue 169, pages 61–66, 1933.
- [6] N. Mariaule. *On the decidability of the p -adic exponential ring*. PhD thesis, University of Manchester, 2013.
- [7] N. Mariaule. Effective model-completeness for p -adic analytic structures. <http://arxiv.org/abs/1408.0610>, 2014.
- [8] A. Wilkie. Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function. *J. Amer. Math. Soc.* 9, No. 4, pages 1051–1094, 1996.